

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

3063 N. 8th St. Milwaukee, Wisconsin 53206, to include all associated common detached garage, and a **Yellow 2007 Hummer H3 bearing Wisconsin license plate ATR 1175**. The property at 3063 N. 8th St. is described as a beige, two-story duplex residence, with white trim and a brown roof. The front door is brown with a black metal gate and includes the numbers “3063” above it. The structure is on the northwest corner of N. 8th St., near W. Burleigh St. The upper unit of the duplex is 3063 N. 8th St.; The lower unit of the duplex is 3061 N. 8th St. There are balconies located in the front and rear of the upper unit. The main entrance is on the east side of the duplex, off the front porch; a second entrance is located on the south side of the duplex, leading to the side yard. A concrete slab and detached garage are located behind the duplex connected to an alley, which can be accessed by W. Burleigh St. and W. Chambers St.



ATTACHMENT B

Property to Be Seized

1. All records relating to violations of 18 U.S.C. § 545 – Smuggling Goods into the United States; 18 U.S.C. § 922(a)(1)(A) – Unlicensed Importation of a Firearm in Foreign Commerce; and 18 U.S.C. § 922(g)(1) – Felon in Possession of a Firearm involving Kirk MICKELSON, including:

- a. Firearm suppressors, and any firearm as defined by 26 U.S.C. §5845(a) that is not lawfully possessed in accordance with the National Firearm Act (NFA) and registered on the National Firearm Transfer Record (NFTR) as required by law.
- b. Any firearm(s), ammunition or other items that are prohibited for certain individuals, including non-citizen aliens, to possess as defined in 18 U.S.C. § 921.
- c. Any items pertaining to the possession, manufacture, or distribution of illegal firearms, including but not limited to, lower receivers, upper receivers, grips, stocks, magazines, trigger assemblies, machinegun conversion kits, and barrels for Glock-style firearms.
- d. Documentation of firearms, firearm transactions, firearm parts, large sums of money and/or co-conspirators and paperwork showing the purchase, storage, disposition, or dominion and control over any illegal firearms, illegal firearm parts, and machinegun conversion kits.
- e. Personal telephone books, telephone records, telephone bills, address books, correspondence, notes, and papers containing names and/or telephone numbers that tends to establish communication between sellers or purchasers or illegal firearms.
- f. Indicia of occupancy, residency, and/or ownership of the items noted above and of the premises, including but not limited to, papers, correspondence, canceled envelopes, canceled postcards, bills, and

registration documents.

- g. Any machines, tools, parts, or other items associated with the use, manufacture, or modification of firearms; firearm parts; Glock lower frames (including firearm variant frames or receivers of any kind); machineguns and machinegun parts, including but not limited to templates, machinegun conversion kits, cutting programs, diagrams, instruction manuals, pamphlets, or other tutorial material regarding the manufacture of firearms and machine guns.
- h. Mailing labels, packaging materials, envelopes, and or parcels relating to the mailing, transportation, ordering, making, purchasing, selling and or unlawful importation of firearms or firearm parts into the United States.
- i. Books, records, receipts, notes, ledgers, contracts, and/or other papers relating to the mailing, transportation, ordering, making, purchasing, selling, and/or unlawful importation of firearms or firearm parts.
- j. All computers and computer hardware, including all cellular telephones, smart phones, tablets, and external hard drives, and computer software, computer- related documentation, and storage media, limited to searching for items described above. Off-site searching of such hardware, software, documentation, and storage media may be conducted and shall be limited to searching for the items described above and shall be done according to the procedures set out below.
- k. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;
- l. international shipping centers,
- m. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

2. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computers, cellular telephones, or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Target Premises and other locations as described in Attachment A, law enforcement personnel are authorized to press the

fingers (including thumbs) of MICKELSON and/or others present to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone, Android, Tablet, or any other device requiring biometric identification, found at the premises for the purpose of attempting to unlock the device via fingerprint or iris scan, in order to search the contents as authorized by this warrant. If facial recognition is required, the subject(s) will remain still and look, with eyes open, at the camera for any device seized in connection with this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 24-897M(NJ)

3063 N. 8th St. Milwaukee, Wisconsin 53206, to include detached
garage, and a Yellow 2007 Hummer H3 bearing Wisconsin license
plate ATR 1175, as further described in Attachment A

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 545; 922(a)(1) (A); and 922(g)(1)	Smuggling Goods into the United States; Unlicensed Importation of a Firearm in Foreign Commerce; and Felon in Possession of a Firearm.

The application is based on these facts:

See Attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

LEIGHTON J MUDEL

Digitally signed by LEIGHTON J
MUDEL
Date: 2024.09.10 11:07:49 -05'00'

Applicant's signature

Leighton Mudel, HSI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 9/10/2024

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Leighton Mudel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following locations and items to include the following, if present, at the locations further detailed in Attachment A, for the items described in Attachment B:

- a. the residence located at **3063 N. 8th St. Milwaukee, Wisconsin 53206**: the “Target Property” herein; and
- b. a **yellow Hummer H3 bearing Wisconsin license plate ATR 1175** if located on the Target Property or parked on a public street within 100 feet of the Target Property: the “Target Hummer” herein.

2. Your affiant is a Special Agent (SA) with Homeland Security Investigations (HSI) and has been so employed since January of 2023. Before that time, was an officer with Customs and Border Protection (CBP) from May of 2021 until January of 2023. In my capacity as an HSI SA, your affiant has investigated various federal crimes, including violations of 18 U.S.C. § 545 – Smuggling Goods into the United States; 18 U.S.C. § 922(a)(1)(A)- Unlicensed Importation of a Firearm in Foreign Commerce; 18 U.S.C. § 922(g)(1) – Felon in Possession of a Firearm as well as other federal violations. During my career in law enforcement, your affiant has investigated violations of federal narcotics laws and related violations, including federal firearm offenses. Based on my training, experience, and participation in firearm related investigations, I am familiar with the

appearance, mechanisms, and operations of various types of firearms. I am also familiar with the appearance, mechanisms, and operations of various types of firearm accessories, including firearm suppressors, which are commonly disguised as “oil filters” when imported illegally. From my training and experience, I know that traffickers of firearms and firearm accessories often use various communication devices to conduct trafficking operations, and that traffickers often communicate on cell phones using text messages and direct connect cell phone capabilities as well as electronic devices to maintain records of purchases, sales, costumers, other co-conspirators, etc. In addition, such communication devices are used to track inventory and/or profits from such illegal activities. I know that firearm and firearm accessory traffickers commonly have in their possession, at their residences, and other locations where they exercise dominion and control: firearms; firearm accessories; ammunition; and records or receipts pertaining to such.

3. In addition, I know from my training and experiences that individuals involved in the illegal importation, sale, or possession of suppressors often will secrete items with evidentiary value in storage facilities and/or vehicles on or near the property where they live, so as to conceal them from law enforcement and/or to protect their valuable illegal items, money, and records from being taken by customers or those they deem their competition.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the

requested warrant and does not set forth all my knowledge about this matter.

5. Based upon the evidence gathered to date, I submit that there is probable cause to believe that Kirk MICKELSON (DOB XX/XX/1989) and other co-conspirators, have committed the following violations: 18 U.S.C. § 545 – Smuggling Goods into the United States; 18 U.S.C. § 922(a)(1)(A) – Unlicensed Importation of a Firearm in Foreign Commerce; and 18 U.S.C. § 922(g)(1) – Felon in Possession of a Firearm. I further submit that there is probable cause that evidence of these criminal violations will be found at the locations your affiant seeks to search as named in the affidavit as the “Target PREMISES,” the “Target GARAGE,” the “Target HUMMER,” and the “Target ELECTRONIC DEVICES,” as further described below and in Attachment A.

**BACKGROUND OF KIRK MICKELSON, THE INDIVIDUAL WHO RESIDES AT
THE TARGET PREMISES YOUR AFFIANT SEEKS TO SEARCH**

6. On September 28, 2009, MICKELSON was convicted of Possession with Intent to Distribute Marijuana, a felony, in Rock County Circuit Court case number 2009CF254. On February 7, 2014, MICKELSON was convicted of three counts of Felony Bail Jumping in Rock County Circuit Court case number 2013CF1206. On February 7, 2014, MICKELSON was convicted of Felon in Possession of a Firearm, a felony, in Rock County Circuit Court case number 2013CF151. On October 2, 2015, MICKELSON was convicted in Eastern District of Wisconsin case number 14-CR-112 of a Conspiracy to import Methylone into the United States. As detailed in the plea agreement, Mickelson and his co-conspirators were involved in importing Methylone from Chinese sources of supply (SOS) into the Eastern District of Wisconsin and elsewhere. Western Union records

between October 2011 and January 2013 revealed that over \$50,000.00 was sent from Wisconsin to the Chinese SOS for Methylone in 34 transactions including payments by MICKELSON.

7. A search of court records also show MICKELSON is currently on federal supervised release in United States District Court, Eastern District of Wisconsin case number 14-CR-112.

8. According to MICKELSON'S Supervising U.S. Probation Officer, MIKELSON resides at 3063 N. 8th St. Milwaukee, Wisconsin 53206 (the "Target Premises") which is the upper unit of a duplex.

PROBABLE CAUSE

9. Based on my training and experience, your affiant is aware that there is a significant market that has developed in the United States for the importation into the United States of high-quality firearm suppressors from China. Generally, the packages are sent through various international shipping centers such as Dalsey, Hillblom and Lynn, commonly referred to as DHL, and are addressed to named individuals at specific locations in the United States. The senders have been identified as being YBD, JC Machinery Tools Inc., and other companies in China known to CBP and HSI as being exporters of illegal suppressors to the United States. These packages usually weigh between 0.10 and 2.34 kilograms and are falsely labeled as containing "filters" and "purifiers," but once opened under CBP's authority to inspect such suspected parcels¹

coming into the United States from abroad, are found to contain suppressors.

10. In addition, your affiant knows there is a significant illegal market in the United States for firearms, suppressors, and other National Firearms Act (NFA) items which are smuggled into the United States from foreign countries. In addition to the inherent threat posed by firearms and NFA items to the community, these smuggled goods allow individuals to conduct criminal activities and evade law enforcement investigations as such items commonly bear no registration or serial numbers. Furthermore, smuggling firearm suppressors and other NFA items allows individuals importing said items to evade federally regulated import taxes and sell them directly on the street, even to those who are not legally allowed to possess such items. Your affiant knows based on my training, experience, and conversations with other law enforcement partners that firearms suppressor can each sell for approximately \$350 to \$1,500.

11. On or about March 25, 2024, MICKELSON was shipped a parcel from YBD, an entity located in China. The parcel entered the United States on or about March 27, 2024, and subsequently shipped to MICKELSON. The parcel was manifested as a "purifier." Although the parcel was not inspected, based on my training and experience, a package of this size and type of package your affiant believes it likely contained another suppressor.

12. On August 16, 2024, HSI SA Gary Roy received information from CBP in reference to the illegal importation of a parcel containing a suspected firearm suppressor, also known as a silencer. Pursuant to 18 U.S.C. § 921(a)(3) (C) a suppressor or silencer is

a firearm.²

13. CBP notified HSI Milwaukee of a parcel they had seized from the DHL international shipping center located in Oak Creek, Wisconsin and CBP indicated that parcel was shipped by JC Machinery Tools Inc. out of Hong Kong, China on or about August 13, 2024. The parcel (shipment ID# 2904499942) weighed approximately 1.44 kilograms and was manifested as an “oil filter.” The listed recipient was Kirk MICKELSON at the address of 3063 N. 8th St. Milwaukee, Wisconsin 53206.

14. CBP also determined that between March 2024 and August 2024, approximately 20 parcels originating from China were shipped to MICKELSON and/or his live-in girlfriend at the “Target Premises.” Based on your affiant’s training, experience, and familiarity with this investigation your affiant believes this large number of parcels, sent to MICKELSON from China in a 5-month period is consistent with MICKELSON illegally importing contraband from China for the purposes of distribution. All the packages weighed between 0.10 and 2.34 kilograms, were labeled as being “purifiers” and “filters,” and valued at approximately between \$5 and \$90 dollars. As stated above, the street value of such silencers can be as high as \$1,500. Therefore, conservatively, the 20 parcels have a combined value of \$30,000.

15. In addition, CBP has also determined that YBD was the shipper of approximately another 112 CBP seizures between the dates of January 22, 2024, and August 24, 2024. Among these seizures, approximately 99 were firearm suppressors,

² 18 U.S.C. § 921(a)(3) (C) states that “the term ‘firearm’ means....a firearm silencer”.

numerous manifested as “purifiers.” Based on my training and experience, I know that the size of the packages seized, as well as their weight, and the country of origin, that such packages are consistent with the illegal importation of suppressors and were the basis for further inspection conducted by CBP.

16. Your affiant has learned that on August 16, 2024, a shipment was referred for an enforcement inspection by CBP. The CBP ATS Import Cargo system showed that it was manifested as “OIL FILTER SAPRE STAINLESS STEEL F,” and had a declared value of \$50.00. Upon inspection on August 19, 2024, one (1) firearm suppressor kit was discovered within the parcel. Based on the findings, the shipment was seized. The package originated in Hong Kong, China, and had the shipper listed as JC Machinery Tools Inc. The parcel was scheduled to be delivered to Kirk MICKELSON at the “Target Premises.”

17. The inspection of the parcel revealed that the contents of the parcel included a solid metal tube along with smaller metal pieces known as baffles,³ which when assembled, form a suppressor. The suppressor was made of stainless steel. Photos of the suppressor were taken as they were discovered. Once opened the baffles were assembled as seen below:

³ A baffle refers to a device or structure that is specifically designed and implemented to control or redirect the flow of sound.





18. On or about August 16, 2024, MICKELSON contacted DHL asking to pick up the parcel at the DHL facility in Oak Creek, Wisconsin. MICKELSON arrived at the DHL facility at approximately 6:30 pm in an attempt to retrieve the parcel. A DHL employee informed your affiant that when MICKELSON spoke to the employee, MICKELSON identified himself by his true name, showed the employee his tracking number for the package and described the package as being from “JP Machinery.” HSI SAs reviewed security camera footage taken at the DHL facility for that date, and observed at around 6:30 pm, MICKELSON entered and interacted with the DHL employee identified as being the one MICKELSON talked with. The footage also showed MICKELSON on his cell phone and leaving the facility after approximately 10 minutes after he inquired regarding the package.

19. MICKELSON later contacted DHL customer service on August 17, 19, 20, and 21 of 2024 in a continued effort to locate the parcel. Each time, MICKELSON stated that he would be the one to pick up the parcel at the DHL facility.

20. On August 26, 2024, at approximately 4:00 pm, your affiant and SA Roy arrived at the DHL facility where MICKELSON had previously attempted to retrieve parcel (shipment ID# 2904499942) containing a firearm suppressor. Your affiant retrieved video and photographs of MICKELSON's presence within the facility and turned the evidence over to an HSI Criminal Analyst.

21. On August 27, 2024, the HSI Criminal Analyst returned comparison results between social media photographs and the DHL photographs of physical attributes and tattoos, providing a high level of certainty that MICKELSON was depicted at the DHL facility, attempting to retrieve the parcel containing the firearm suppressor.

22. Furthermore, DHL employees provided your affiant with copies of logs made by the customer service department of their interactions with MICKELSON. I observed the logs which, in summary, indicated that MICKELSON called the customer service line for the purpose of locating the package with the suppressor on the above-mentioned dates. MICKELSON identified himself by name and provided his phone number as 414-331-0231. The phone number MICKELSON provided is the same number on the shipping label of the firearm suppressor directly under the contact name of Kirk MICKELSON as can be seen below:

WAYBILL DOC		WPX 	
<small>Not to be attached to package - Hand to Courier 2024-08-16 (Reproduction) / 2024-08-12 (Data)</small>			
Shipper : JC MACHINERY TOOLS INC XIONG ZHIJI ROOM 403 BUILDING 4 1199 FOREST PRO TECTION ROAD HUANGPU DISTRICT IF RTO PLS RTN TO HKG FOR SHPR INST HONG KONG SAR, CHINA		Contact: XIONG ZHIJI/67385053 Reference: 2024081233	
Receiver : KIRK MICKELSON KIRK MICKELSON 3063 N 8TH STREET MILWAUKEE WISCONSIN 53206 USA MILWAUKEE WI 53206 UNITED STATES OF AMERICA		Contact: KIRK MICKELSON 1 4143310231	
HK-HKG-TYC US-MKE-MK1			
Product Details: [P] EXPRESS WORLDWIDE (I) Payer Details FRT A/C No: 631360353		Features / Services (Service Code) Duties and Taxes UnPaid(DS) Paperless Trade(WY)	
DUTY SERVICE IND : DTU			
Shipment Details Account No: 631360353 Ref Code: 2024081233 Customs Value: 50.00 USD Shipment Content: OIL FILTER SAPRE STAINLESS STEEL FILTERATE 1 PCS			
Cust Decl Shpt Wgt (UOM) / Dim Wgt (UOM): 0.5 kg /		Pieces 1	
<small>Name (in Capital Letters)</small>	<small>Signature</small>	<small>Date (DD.MM.YYYY)</small>	
		EEI: ShipperEIN	
WAYBILL 29 0449 9942			
<small>License Plates of pieces in shipment JD014600011687975692</small>			

23. HSI SAs spoke with MICKELSON'S Probation Officer (PO), who provided MICKELSON'S current registered address as being the "Target Premises." MICKELSON'S PO stated the residence is an upper unit and has visited MICKELSON at the address. MICKELSON'S PO stated MICKELSON drives a yellow Hummer which MICKELSON had received from his aunt who has subsequently been identified as being Peggy Sue Stowers.

24. Your affiant conducted records checks in the Department of Transportation (DOT) database. Records indicated that MICKELSON has a current identification card and expired driver's license. Both identities list MICKELSON'S address as the "Target

Premises.”

25. On or about August 29, 2024, your affiant and SA Roy conducted surveillance at 3063 N 8th St, Milwaukee, WI 53206. During surveillance, your affiant observed MICKELSON exit the residence, walk out to a yellow Hummer parked directly in front of the address and retrieve documents from the rear passenger seat. Your affiant observed MICKELSON unlock the Hummer with a key before retrieving the documents. Later, your affiant observed MICKELSON leave the “Target Premises,” and drive away. I observed the yellow Hummer bore Wisconsin license plate ATR 1175.

26. Records checks were conducted in the DOT database which revealed that the Hummer was registered to a Peggy Sue Stowers at the address of 2013 Kenwood Ave, Beloit, WI 53511. A search of the CLEAR database revealed that Peggy Sue Stowers is also known as Peggy Sue Mickelson and is a first-degree relative of MICKELSON. Further, records showed that between January 1, 2024, and July 26, 2024, MICKELSON also listed himself as residing at the 2013 Kenwood Ave address along with Peggy Sue Mickelson.

27. During surveillance, HSI SAs also observed MICKELSON’S yellow Hummer parked in the alley behind the Target Premises directly next to a garage with a red door that is located on the “Target PREMISES.” Your affiant observed that the garage door faces the alley and is connected to the “Target PREMISES” by a wooden fence. Moreover, it appears that in order for MICKELSON to access the ally from the rear of the residence, MICKELSON would have to either go through the garage or exit a gate door. Based on my training and experience the location of this garage is consistent with being a location easily accessible to MICKELSON and as being a location that could be used to hide

contraband, and other evidence of his criminal activity.

28. Further, affiant is aware, based on training, experience, and information provided from other members of law enforcement, that evidence of illegal firearm and firearm accessory possession is commonly found on electronic devices such as computers and cellular phones. Affiant is aware that those engaged in the importation, sale, or possession of firearms and firearm accessories often take, or cause to be taken, photographs, video, and other visual depictions of firearms and firearm accessories, and typically keep and maintain these photographs, video, and other visual depictions in cellular phones located on their person or on other mediums such as computers and hard drives in areas where they have exercised dominion and control.

29. Affiant is aware that it is common for those who possess and/or traffic firearms and firearm accessories, to purchase and maintain ownership of firearms and firearm accessories for long periods of time. This often occurs as they may purchase such items to have them on inventory to sell to clients. Because of the high cost of each suppressor, it is likely to be for long periods of time as the transactions with the Chinese SOS can be delayed for various reasons as can the ability of the intended purchaser may be delayed due to having to raise the money needed to purchase such firearms and firearm accessories.

30. Affiant is aware that cellular phones and other electronic devices can be used to store information including text messages, multimedia messages, and a history of incoming and outgoing calls, contact/address book information, photographs, videos, GPS and other location information, internet search history, and other data relevant to

the illegal activities. Cell phones and electronic devices are also used to take customer orders, track packages, may payments to international delivery companies, and/or to keep track of payments, and receipts as well as other processes used to conduct such business.

31. MICKELSON is prohibited from possessing firearms, firearm suppressors, ammunition, and NFA items due to him being a person previously convicted of a felony offense. In addition, he is prohibited from Smuggling Goods into the United States, in violation of 18 U.S.C. section 545. Further, MICKELSON is not licensed to Import a Firearm or suppressors in Foreign Commerce, in violation of 18 U.S.C. section 922(a)(1)(A).

32. Based on the facts stated herein, there is probable cause to believe that evidence associated with the criminal violations detailed above will be located within the Target Premises, the Targe Storage Area, the Target Hummer, and/or the person(s) of those present at the time of the search, including the person of Kirk MICKELSON.

TECHNICAL TERMS

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term— IP addresses, while other computers have dynamic—that is, frequently

changed— IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

34. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- i. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- ii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- iii. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- iv. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

34. *Forensic evidence.* As further described in Attachment B, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the identified locations in Attachment A because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information

such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional

electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when a person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.
- v. purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media

often requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- iii. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off- site reviewing with specialized forensic tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

37. *Biometric Data.* I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, Samsung, and other manufacturers, that some models of Apple or other manufacturer's devices such as iPhones, Smartphones, and iPads or Tablets offer their users the ability to unlock the device via the use of a biometric access fingerprint or thumbprint (collectively, "fingerprint"); facial recognition feature; and or by use of an iris reader. These devices can be unlocked by having the owner touch, put their face near the device, or show their retinas to the device(s) even if law enforcement does not have the numeric or alphanumeric passcode or password.

38. If a user enables Touch ID for use of a fingerprint access on a given Apple or other manufacturer's device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is

found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device.

39. If a user enables facial recognition (biometric access), he or she can display their face to the device camera of the locked Apple, Samsung, or other device(s) to unlock that device.

40. In my training and experience, users of Apple, Samsung, and other manufacturer’s devices that offer biometric access often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

41. In some circumstances, a fingerprint, facial recognition, or an iris scan cannot be used to unlock a device that has been biometric enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked biometrically in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple or other device, the opportunity to unlock the device biometrically exists for only a short time. Further, biometric access will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device biometrically have been made.

42. If biometric enabled Apple, Samsung, or other manufacturer’s devices are

found during a search of the locations subject to this warrant, the passcode or password that would unlock such the devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of any device(s) found during the search of the location to the device's Touch ID sensor or hold the device up to the user(s)' face or the user(s) eye in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) with the use of the biometric information is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

43. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometrics, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the location or vehicle searched to press their finger(s) against the Touch ID sensor or display their face to the device camera of the locked device(s) found during the search of the location in order to attempt to identify the device's user(s) and unlock the device(s) by its biometric

capability.

CONCLUSION

44. Based on the facts as stated above, I submit that this affidavit supports probable cause for a warrant to search the PREMISES and person of Kirk MICKELSON (DOB XX/XX/1989), described in Attachment A, and seize the items described in Attachment B.

ATTACHMENT A

Property to Be Searched

3063 N. 8th St. Milwaukee, Wisconsin 53206, to include all associated common detached garage, and a **Yellow 2007 Hummer H3 bearing Wisconsin license plate ATR 1175**. The property at 3063 N. 8th St. is described as a beige, two-story duplex residence, with white trim and a brown roof. The front door is brown with a black metal gate and includes the numbers “3063” above it. The structure is on the northwest corner of N. 8th St., near W. Burleigh St. The upper unit of the duplex is 3063 N. 8th St.; The lower unit of the duplex is 3061 N. 8th St. There are balconies located in the front and rear of the upper unit. The main entrance is on the east side of the duplex, off the front porch; a second entrance is located on the south side of the duplex, leading to the side yard. A concrete slab and detached garage are located behind the duplex connected to an alley, which can be accessed by W. Burleigh St. and W. Chambers St.



ATTACHMENT B

Property to Be Seized

1. All records relating to violations of 18 U.S.C. § 545 – Smuggling Goods into the United States; 18 U.S.C. § 922(a)(1)(A) – Unlicensed Importation of a Firearm in Foreign Commerce; and 18 U.S.C. § 922(g)(1) – Felon in Possession of a Firearm involving Kirk MICKELSON, including:

- a. Firearm suppressors, and any firearm as defined by 26 U.S.C. §5845(a) that is not lawfully possessed in accordance with the National Firearm Act (NFA) and registered on the National Firearm Transfer Record (NFTR) as required by law.
- b. Any firearm(s), ammunition or other items that are prohibited for certain individuals, including non-citizen aliens, to possess as defined in 18 U.S.C. § 921.
- c. Any items pertaining to the possession, manufacture, or distribution of illegal firearms, including but not limited to, lower receivers, upper receivers, grips, stocks, magazines, trigger assemblies, machinegun conversion kits, and barrels for Glock-style firearms.
- d. Documentation of firearms, firearm transactions, firearm parts, large sums of money and/or co-conspirators and paperwork showing the purchase, storage, disposition, or dominion and control over any illegal firearms, illegal firearm parts, and machinegun conversion kits.
- e. Personal telephone books, telephone records, telephone bills, address books, correspondence, notes, and papers containing names and/or telephone numbers that tends to establish communication between sellers or purchasers or illegal firearms.
- f. Indicia of occupancy, residency, and/or ownership of the items noted above and of the premises, including but not limited to, papers, correspondence, canceled envelopes, canceled postcards, bills, and registration documents.

- g. Any machines, tools, parts, or other items associated with the use, manufacture, or modification of firearms; firearm parts; Glock lower frames (including firearm variant frames or receivers of any kind); machineguns and machinegun parts, including but not limited to templates, machinegun conversion kits, cutting programs, diagrams, instruction manuals, pamphlets, or other tutorial material regarding the manufacture of firearms and machine guns.
- h. Mailing labels, packaging materials, envelopes, and or parcels relating to the mailing, transportation, ordering, making, purchasing, selling and or unlawful importation of firearms or firearm parts into the United States.
- i. Books, records, receipts, notes, ledgers, contracts, and/or other papers relating to the mailing, transportation, ordering, making, purchasing, selling, and/or unlawful importation of firearms or firearm parts.
- j. All computers and computer hardware, including all cellular telephones, smart phones, tablets, and external hard drives, and computer software, computer- related documentation, and storage media, limited to searching for items described above. Off-site searching of such hardware, software, documentation, and storage media may be conducted and shall be limited to searching for the items described above and shall be done according to the procedures set out below.
- k. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;
- l. international shipping centers,
- m. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

2. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have

been created or stored, including any form of computers, cellular telephones, or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;

- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Target Premises and other locations as described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of MICKELSON and/or others present to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone, Android, Tablet, or any other

device requiring biometric identification, found at the premises for the purpose of attempting to unlock the device via fingerprint or iris scan, in order to search the contents as authorized by this warrant. If facial recognition is required, the subject(s) will remain still and look, with eyes open, at the camera for any device seized in connection with this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.